Lightweight Error Correction Technique in Industrial IEEE802.15.4 Networks

F. Civerchia*, E. Rossi†, L. Maggiani†‡, S. Bocchino†‡, C. Salvadori†‡, and M. Petracca†‡
*New Generation Sensors S.r.l., Pisa, Italy
†Scuola Superiore Sant'Anna di Pisa, Pisa, Italy
‡Scuola Superiore Sant'Anna Research Unit, National Inter-University Consortium for Telecommunications, Pisa, Italy
Email: [federico.civerchia]@ngs-sensors.it, [en.rossi|l.maggiani|s.bocchino|c.salvadori|m.petracca]@sssup.it

***Abstract*—Industrial Wireless Sensor Networks (IWSNs) are nowadays becoming more and more popular thanks to their flexibility and pervasive monitoring capabilities to support process automation and remote maintenance applications. In such a scenario, channel errors due to the wireless medium can result in data packet losses, and consequently in unreliable IWSN services.**

To mitigate the above reported problem, this paper presents a lightweight error correction scheme specially developed for IEEE802.15.4-based IWSNs. By adding error correction and detection information inside the IEEE802.15.4 MAC data frame, the proposed FEC scheme is able to guarantee a backward compatibility with the standard while providing advanced capabilities in recovering data packets affected by bit errors. In the paper the benefits of the proposed technique are first evaluated through simulated loss traces, then they are validated in a real environment by considering real loss traces collected in an electricity power plant. The proposed error correction scheme is able to recover around 50% of the data packets that would be lost in case of a standard communication without any error correction capability.

I. Introduction

Wireless Sensor Networks (WSNs) are nowadays largely adopted in industrial environments thanks to their flexibility and pervasive monitoring capabilities able to successfully support process automation, remote maintenance, and advanced applications [1], [2]. Despite the great benefit carried out by this technology, wireless communications in industrial environments are challenging regarding communication reliability [3]. Obstacles, ferrous materials, moving objects and other sources of electromagnetic interference can result in packet errors, and consequently on unreliable wireless based services. To reduce data losses in a wireless scenario two techniques are mainly adopted: Automatic Repeat reQuest (ARQ) and Forward Error Correction (FEC).

ARQ is an error recovery technique based on the retransmission of data packets after an explicit (i.e., formal request trough a dedicated message) or implicit (i.e., no reception of an acknowledgment frame) request from the receiver node. In FEC techniques, instead, reliability is provided by adding redundant information to original data. In an Industrial WSN (IWSN) scenario based on pervasive and constrained monitoring devices, the use of redundant packets can result in network congestions with the risk of a possible block of all monitoring services [4]. On the contrary, FEC techniques can avoid the above mentioned problem although they require an additional computation overhead due to the evaluation of the redundant information to be added inside the data packet. Considering IEEE802.15.4-based [5] IWSNs, the low-level reference standard used in WirelessHART and ISA100.11a systems [6], few FEC-based techniques have been proposed over the years. In [7], and in its enhanced version [8], a FEC-based technique to be implemented at Media Access Control (MAC) layer is proposed by considering Reed Solomon (RS) and Bose and Ray-Chaudhuri (BCH) codes to protect both header fields and payload. In both works the backward compatibility with the IEEE802.15.4 standard is maintained, as well as an increased communication reliability is achieved at the cost of an additional overhead in terms of computational power for data decoding purposes. In order to improve the communication reliability, new classes of error correction codes are nowadays considered for the wireless sensor network scenario. Turbo codes and Low Density Parity Check (LDPC) codes are largely investigated by proposing lightweight coding and decoding techniques to be used in constrained devices [9]. However, although their use has proven to reduce packet errors, such codes fail to fulfill both memory and timing requirements in real devices used in the IWSN scenario, as reported in [10] by Yitbarek et al. According to the same work the most lightweight approaches for FEC techniques in IEEE802.15.4-based networks are based on Repetition and Hamming codes, though they do not reach the same error recovery performance of RS codes (RS(15,11) is identified as the best solution).

In this work we propose a MAC layer based FEC technique targeted to IEEE802.15.4 industrial wireless sensor networks, and able to guarantee a backward compatibility with the standard. By considering next generation IWSNs following the Internet of Things (IoT) vision in which smart devices running complex algorithms will be pervasively deployed in the field for control and maintenance applications, the proposed technique aims at reducing coding and decoding complexity by using Repetition codes and a fast error detection process already defined in the IEEE802.15.4 standard and implemented in hardware in popular transceivers. By reducing the complexity related to error correction, ideally moving all the computation in the transceiver, advanced algorithms can be implemented in smart devices without searching strong trade-offs between onboard application logic performance and

978-1-5090-3474-1/16/$31.00 ©2016 IEEE

possible optimizations related to network communications.

The rest of the paper is structured as follows. The proposed FEC scheme is described in Section II after recalling some details about the IEEE802.15.4 data packet composition. Section III details the performance of the proposed FEC strategy, and it is organized into two main parts. In the first part performance are presented through simulations in which channel errors are simulated by using the Gilbert-Elliot channel error model [11], [12]. In the second part, a data collection activity in a real industrial scenario is reported by analyzing both Bit Error Rate (BER) and average Burst Length (BL) in several communication links. Moreover, collected traces are used to evaluate packet losses with and without the proposed FEC scheme. Section IV concludes the paper.

II. Proposed error correction technique

This section first details IEEE802.15.4 specifications in data packet composition and error detection capabilities, then introduces the proposed MAC layer based FEC scheme by reporting the error correction algorithm.

A. IEEE802.15.4 standard

The IEEE802.15.4 standard in its specifications defines both Physical and MAC layers according to the ISO/OSI protocol stack model. At MAC layer four main protocol data units are defined: (i) beacon frame, (ii) ack frame, (iii) command frame, and (iv) data frame. Since FEC techniques are usually applied to the data frame only, in the following of the section only the data frame is detailed by reporting its main fields.

Fig. 1 shows the IEEE802.15.4 data packet in case no MAC layer based security is used. The packet header is composed by three main fields: (i) frame control, (ii) sequence number, and (iii) addressing fields. In the considered case the maximum header size is equal to 23 bytes. The data payload has a maximum dimension of 102 bytes, and it is followed by a Frame Check Sequence (FCS) field which has a length of 2 bytes. The maximum IEEE802.15.4 data packet dimension results equal to 127 bytes.

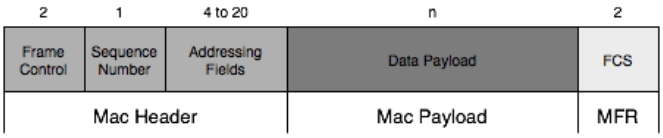

Fig. 1: Standard IEEE802.15.4 data frame without Auxiliary Security Header fields.

The FCS field contains a 16-bit ITU-T CRC and is calculated over the MAC header and payload parts of the frame for error detection purposes. Once a data packet is received, the receiver node evaluates the FCS value again, and in case there is a mismatch between received and evaluated values the packet is discarded because affected by bit errors. The FCS evaluation can be easily implemented in hardware [13].

B. FEC scheme

As previously introduced, the proposed MAC layer based FEC technique is targeted to low-complexity, and it is mainly based on Repetition codes with fast error detection capabilities. Since one of the main requirements is the backward compatibility with the IEEE802.15.4 standard, the proposed technique does not introduce new MAC frames or modifications in the MAC data frame structure, but it proposes a way to use the MAC data packet payload by adding the required information for error correction. In this way, devices or transceivers implementing the FEC scheme can start the error correction procedure after assessing a difference in the received and evaluated FCSs, while other nodes which are not aware of the whole error correction method can discard the data packet because of errors. The proposed FEC scheme is graphically depicted in Fig. 2.

Fig. 2: Standard IEEE802.15.4 data frame with data payload fields required by the proposed FEC scheme.

In the MAC payload, the last 2 bytes are used to send the FCSH field, an FCS value evaluated over the header only. Since we decided not to recover header errors to save available bytes for data, such field is required to understand whether the header is corrupted or not with a consequent discard of the packet. Data to be sent (Dx) are first completed with an additional FCS field (FCSx), and then repeated inside the payload three times. The additional FCS field evaluated on data only is a strong and simple error detection enforcement that can be used at the receiver side to understand whether a repeated data block is corrupted or not. The first data block without errors is used as received data to be used in device applications or to correct the other data blocks in case of multi-hop communications. Such approach avoids a majority voting in repetition coding by leveraging on the additional FCS fields. Since the FEC technique is targeted to IWSNs in which both process automation and remote maintenance applications are supported, in case all the three blocks of data result corrupted the packet is discarded. The whole envisioned scheme requires evaluating two more FCS values (i.e., FCSH, and FCSx) before sending the packet. By using the same 16-bit ITU-T CRC algorithm defined by the standard, the additional FCS fields can be easily evaluated in hardware. At the receiver side, up to five FCS values can be evaluated according to the error correction algorithm reported in Algorithm 1. In the algorithm pseudocode, the received data block after all bit errors have been recovered is labeled as D_{rx}, and the FCS values calculated at the receiver side and in the data packet are labeled with rx and tx respectively. Considering the IEEE802.15.4 MAC data frame length reported in Section II-A, no security applied, the maximum available

data block dimension able to avoid the fragmentation of the information in several packets is equal to 31 bytes. When a security header field is inserted, a lower number of bytes can be sent. For instance with additional 14 bytes for security the maximum available data block dimension able to avoid the fragmentation is equal to 26 bytes. Such a data size dimension is enough for a wide range of monitoring applications in the industrial environment. Temperature, vibration analysis results, and other sensor outputs can be easily accommodated in the maximum available block.

Algorithm 1 Error correction algorithm

```
Evaluate FCS_rx
if FCS_rx is equal to FCS_tx then
    D_rx is equal to D_1
else
    Evaluate FCSH_rx
    if FCSH_rx is not equal to FCSH_tx then
        Discard the packet
    else
        Evaluate FCS1_rx, FCS2_rx, FCS3_rx
        if FCSi_rx is not equal to FCSi_tx (i=1,2,3) then
            Discard the packet
        else
            D_rx is equal to D_i where i is the index of the data
            block which has FCSi_rx is equal to FCSi_tx
        end if
    end if
end if
```

III. Performance evaluation

The performance of the proposed FEC scheme is reported in this section considering both simulations and real loss traces collected in an electricity power plant. In the former case, the channel error model is briefly introduced before presenting Packet Loss Rate (PLR) based performance. In the latter case, the data collection setup is briefly presented before reporting statistics on the channel behavior and PLR performance with and without the proposed FEC scheme. In all presented results the PLR with and without protection have been evaluated by using a simulator able to read loss traces (simulated or real), and apply or not the protection scheme.

A. Performance with simulated loss traces

The performance of the proposed FEC strategy has been analyzed through simulations by using a two-stage Gilbert-Elliot [11], [12] error model. According to such a model the wireless channel is modeled with a two-state Markov chain characterized by good and bad states. In each state a bit error probability can be imposed, thus modeling the effects of possible interference. However, the model requires that possible bit flips in the good state happen sporadically, while the majority occurs in the bad state. Starting from the transition probabilities of the model the mean state sojourn time can be evaluated, as well as the global bit error rate. Each state sojourn time results geometrically distributed. Under the condition that bit flips can occur in the bad state only, the global BER is proportional on the time spent in the bad state, while the average time, in the number of bits, spent in the bad state is equal to the average burst length. As a consequence, by imposing the bit error rate and the imposed average burst length, the whole error channel model is characterized. In Table I results of the performed study are reported as a function of the block data size D, the BER, and considering the average BL equal to 2.5 bits. In each simulation the dimension of the packet in case of no FEC technique is applied, is the sum of the header size (23 bytes), the data size D, and the FCS (2 bytes). When the proposed FEC scheme is applied the packet size is due to the sum of the header, the three repetition of D, the four added FCSs and the global FCS. The data size D ranges from 4 to 28 bytes in order to consider applications in which multiple floating-point data are sent in the same packet to save energy. For instance, this is the case in which a high precision temperature sensor is used and up to seven values are sent in the same data packet. From reported results, the benefit of the proposed FEC scheme can be easily noticed for high values of BER (equal to 10^{-3} and 10^{-4} in the simulations) and D, where almost half of data packets previously discarded are now recovered. By decreasing the data size, still considering high BER values, the FEC scheme error recovering gain decreases accordingly. In the case of BER values lower than 10^{-5} the PLR reduction of the FEC strategy is minimal, even though it is still effective in recovering bit errors.

TABLE I: PLR results with and without FEC scheme as a function of BER and data size D in a simulated environment.

D	**PLR no FEC (%)**			**PLR FEC (%)**		
	BER			BER		
	10^{-3}	10^{-4}	10^{-5}	10^{-3}	10^{-4}	10^{-5}
28	15.69	1.69	0.17	8.00	0.81	0.08
24	14.59	1.56	0.15	7.97	0.81	0.08
20	13.49	1.43	0.14	7.94	0.81	0.08
16	12.36	1.31	0.13	7.90	0.81	0.08
12	11.24	1.17	0.11	7.89	0.81	0.08
8	10.09	1.05	0.11	7.85	0.80	0.08
4	8.93	0.93	0.09	7.83	0.80	0.08

B. Performance with real loss traces

In order to prove the benefits of the proposed technique in a real industrial environment, several loss traces have been collected in an electricity power plant. To this end, real devices equipped with IEEE802.15.4-based transceivers have been used and programmed to send predefined data packets towards a receiver node able to receive both good and corrupted frames.

All received data are then stored in an external device through a serial communication to perform off-line data analysis. The reference hardware used in the whole data collection campaign is the Seed-Eye board [14], an embedded device mounting a Microchip PIC32 microcontroller, the Microchip MRF24J40MB transceiver reaching a maximum transmission power of +20dBm, and a large number of communication buses to be used to connect external sensors. During the campaign, the loss traces have been collected by moving the sending device in several positions of the power plant located on three different floors, while the receiver node has been kept fixed in a position close to a possible control room of the system. A picture of the receiver node connected to the storage system is reported in Fig. 3, while several installations for the sender node are reported in Fig. 4. The total number

Fig. 3: Receiver node with external storage system.

of tested positions is equal to 9, and they have been chosen in order to have different propagation conditions (presence or absence of ferrous material and occlusions). Moreover, each floor is separated by a metal grid, and the maximum distance between the sender and the receiver is approximately 40 m. For each position thousand packets have been sent in several runs in order to filter out possible time-varying wireless channel fluctuations, while the transmission power has been imposed equal to +20dBm, the maximum allowed value according to the ETSI EN 300 328 specifications [15]. All results related to the data collection campaign are reported in Table II, where for each position have been reported the BER and BL values extracted from a post-processing analysis of all collected traces, as well as the PLR obtained with and without the proposed FEC scheme. A data size D equal to 28 bytes has been considered.

In the considered industrial scenario the BER ranges from a minimum of $1.2 \cdot 10^{-6}$ to a maximum of $5.2 \cdot 10^{-4}$, with BL values up to 2.6. In any position the proposed FEC scheme is able to recover at least half of data packets discarded in case no FEC policy is applied, thus showing its benefits in enhancing wireless-based applications reliability in real environments.

TABLE II: PLR results with and without FEC scheme considering real loss traces collected in an electricity power plant.

Position	**BER**	**BL [bits]**	**PLR no FEC (%)**	**PLR FEC (%)**
1	$2.5 \cdot 10^{-5}$	1.3	0.84	0.40
2	$5.2 \cdot 10^{-4}$	1.7	12.10	5.97
3	$5.2 \cdot 10^{-5}$	1.6	1.41	0.68
4	$2.1 \cdot 10^{-6}$	1.0	0.10	0.05
5	$2.8 \cdot 10^{-5}$	2.6	0.44	0.23
6	$1.2 \cdot 10^{-6}$	1.0	0.05	0.02
7	$3.6 \cdot 10^{-6}$	1.0	0.14	0.07
8	$2.8 \cdot 10^{-5}$	2.0	0.63	0.30
9	$1.8 \cdot 10^{-4}$	1.7	4.40	1.16

IV. Conclusions and Future Work

In the paper, a lightweight error correction scheme targeted to industrial wireless sensor networks based on the IEEE802.15.4 standard is presented. The proposed FEC scheme is mainly based on Repetition codes and it is supported by a fast error detection process based on the evaluation of frame check sequence values both on packet header and blocks of data. By adding additional data information and error detection fields in the payload of the standard IEEE802.15.4 MAC data frame, the proposed technique is able to guarantee a backward compatibility while providing advanced features in recovering data packets affected by bit errors.

The performance of the proposed FEC scheme has been evaluated through simulations considering both simulated and real loss traces collected in an electricity power plant. In both cases the technique shows its effectiveness in correcting bit errors by guaranteeing to recover around 50% of data packets that would be lost without any error correction technique, thus showing its benefits in enhancing communication reliability to fully support process automation and remote maintenance applications in the reference scenario.

Future works in this research area will consider the introduction of an additional channel error model able to characterize interference in the reference frequency band, thus allowing a fair comparison with other FEC-based techniques already proposed in the literature. Moreover, the effect of errors in the packet header will be investigated to understand under which conditions a redundancy scheme on the header can be necessary.

References

[1] M. Erdelj, N. Mitton, and E. Natalizio, "Applications of industrial wireless sensor networks," in *Industrial Wireless Sensor Networks*, chapter 1, pp. 1–22. CRC Press, London, USA, April 2013.

[2] M. Petracca, S. Bocchino, A. Azzarà, R. Pelliccia, M. Ghibaudi, and P. Pagano, "WSN and RFID Integration in the IoT scenario: an Advanced safety System for Industrial Plants," *Journal of Communications Software and Systems*, vol. 9, no. 1, pp. 104–113, March 2013.

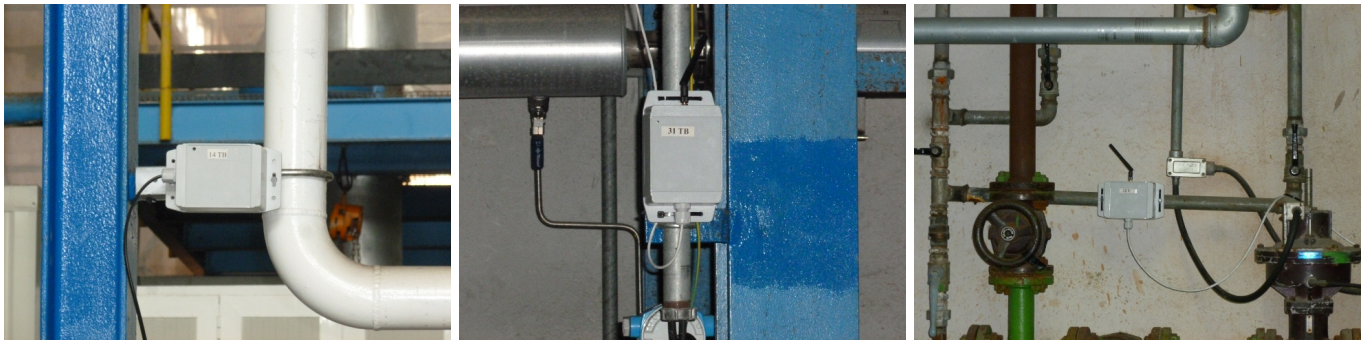

Fig. 4: Sender node installed in several positions inside the electricity power plant.

[3] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, October 2009.

[4] J. Åkerberg, M. Gidlund, F. Reichenbach, and M. Björkman, "Measurements on an industrial wireless hart network supporting profisafe: A case study," in *Conference on Emerging Technologies Factory Automation*, September 2011, pp. 1–8.

[5] IEEE Computer Society, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPAN)," *The Institute of Electrical and Electronics Engineers, Inc.*, October 2003.

[6] D. Yang, Y. Xu, and M. Gidlund, "Coexistence of ieee802.15.4 based networks: A survey," in *Annual Conference of IEEE Industrial Electronics Society*, November 2010, pp. 2107–2113.

[7] K. Yu, M. Gidlund, J. Akerberg, and M. Bjorkman, "Reliable and low latency transmission in industrial wireless sensor networks," *Procedia Computer Science*, vol. 5, pp. 866 – 873, 2011.

[8] K. Yu, F. Barać, M. Gidlund, J. Åkerberg, and M. Björkman, "A flexible error correction scheme for ieee 802.15.4-based industrial wireless sensor networks," in *IEEE International Symposium on Industrial Electronics*, May 2012, pp. 1172–1177.

[9] G.Biroli, M. Martina, and G. Masera, "An ldpc decoder architecture for wireless sensor network applications," *Sensors*, vol. 2, no. 12, pp. 1529 – 1543, 2012.

[10] Y. H. Yitbarek, K. Yu, J. Åkerberg, M. Gidlund, and M. Björkman, "Implementation and evaluation of error control schemes in industrial wireless sensor networks," in *IEEE International Conference on Industrial Technology*, February 2014, pp. 730–735.

[11] E. N. Gilbert, "Capacity of a burst-noise channel," *Bell System Technical Journal*, vol. 39, no. 5, pp. 1253–1265, 1960.

[12] J.P. Ebert and A. Willig, "A Gilbert-Elliot Bit Error Model and the Efficient Use in Packet Level Simulation," Tech. Rep., Technical University Berlin, March 1999.

[13] Microchip Technology Inc., *MRF24J40 Data Sheet IEEE802.15.4 2.4 GHz RF Transceiver*, 2010, Rev. C.

[14] B. Dal Seno, M. Ghibaudi, and C. Scordino, "Embedded boards for traffic monitoring," in *Poster session of the IPERMOB project final workshop*, www.ipermob.org/files/DemoSAT/afternoon/2011-05-18_poster_hw_oo3.pdf, May 2011.

[15] European Telecommunications Standards Institute, "ETSI EN 300 328 v1.7.1," 2006.